SOME RELATIONS BETWEEN SUBSTITUTION GROUP PROPERTIES AND ABSTRACT GROUPS.

By G. A. MILLER.

(*Received June 4, 1910.*)

Dyck observed that the necessary and sufficient condition that a transitive substitution group G of degree n is primitive is that its subgroup G_1 which is composed of all the substitutions of G which omit one letter is a maximal subgroup of G[1]. This establishes an important relation between primitive substitution groups and the properties of G considered as an abstract group. It has also been observed that abstract group properties correspond to the different degrees of transitivity of substitution groups[2], and that the number of ways in which an abstract group can be represented as a transitive substitution group can be directly deduced from the properties of the group. These and other known relations have done much towards uniting the theories of abstract groups and those of substitution groups, and towards making these theories mutually helpful. It is the object of the present paper to establish other important relations between these two theories, especially as regards abstract groups and simply transitive substitution groups.

§ 1. *Some properties of co-sets.*

If H represents any subgroup of index ρ under a group G all the operators of G may be arranged so as to give ρ distinct sets both as regards right-hand and as regards left-hand multiplication, in the following forms:[3]

$$G = H + HS_2 + HS_3 + \ldots + HS_\rho,$$
$$= H + S_2H + S_3H + \ldots + S_\rho H.$$

[1] *Mathematische Annalen*, vol. 22 (1883), p. 94.
[2] *Messenger of Mathematics*, vol. 28 (1899), p. 107.
[3] *Bulletin of the American Mathematical Society*, vol. 16 (1910), p. 454.

The sets HS_α, $S_\alpha H$ $(\alpha = 2, 3, \ldots, \rho)$ are known as *co-sets* of G as regards H. Galois called attention to the importance of the case when each $HS_\alpha = S_\alpha H$ for every operator of H. That is, for every operator of H in the first member there is some operator of H in the second member so that this equation may be satisfied. The necessary and sufficient condition that H is invariant under G is that such equations may be established for every value of α from 2 to ρ.

The co-sets HS_α. $S_\alpha H$ will be called right and left co-sets respectively. The totality of these co-sets is independent of the choice of the operators $S_2, S_3, \ldots, S$; that is, there is only one category of right co-set, and only one of left co-sets as regards any given subgroup. Each left co-set is composed of the inverses of all the operators in a right co-set and vice versa. Hence we may say that the necessary and sufficient condition that a subgroup H is invariant under a group G is that every right co-set of G as regards H is identical with some left co-set as regards H, or that every left co-set is identical with some such right co-set. In other words, the necessary and sufficient condition that H is invariant under G is that the number of distinct co-sets to which H gives rise is equal to its index under G diminished by unity, or that the totality of its right co-sets is identical with the totality of its left co-sets. This theorem is included in the theorem that the necessary and sufficient condition that H is invariant under a right co-set is that this co-set is identical with some left co-set, or vice versa.

With the extreme case in which each right co-set is identical with some left co-set we may contrast the other extreme case when each right co-set has some operator in common with every left co-set. It has been seen that H is invariant in the first case and we shall see that it gives rise to a multiply transitive substitution group (K)[4] in the second case, excluding the trivial case when the order of K is 2. In the proof of this theorem it will at first be assumed that H is neither invariant under G nor does it involve any invariant subgroup of G besides the identity. That is, we shall at first assume that K is a transitive substitution group which is simply isomorphic with G.

[4] Dyck, *Mathematische Annalen*, vol. 22 (1883), p. 91.

The subgroup (K_1) which is composed of all the substitutions of K which omit a given letter a is simply isomorphic with H. Hence the co-sets of G as regards H have the same properties as the co-sets of K as regards K_1. In the latter case, each of the right co-sets is composed of all the substitutions of K which replace a by the same letter, while each of the left co-sets replaces a by all the letters of a system of intransitivity of K_1. Hence it results that in this case the necessary and sufficient condition that K is multiply transitive is that each right co-set as regards K_1 has at least one operator in common with every left co-set.

When H is invariant under G it results that K is a regular group and the theorem given above requires no proof since a regular group cannot be multiply transitive. When H involves an invariant subgroup of G but is not itself invariant under G, K will be the quotient group of G with respect to the maximal invariant subgroup of H which is also invariant under G. It is evident that the reasoning employed above applies directly to this quotient group, and hence we have proved the following theorem: *The necessary and sufficient condition that a given subgroup of a group gives rise to a multiply transitive representation of the group, or of one of its quotient group whose order exceeds two, is that every right co-set with respect to this subgroup has at least one operator in common with every left co-set with respect to the same subgroup.* This theorem may also be stated as follows: the necessary and sufficient condition that H gives rise to a multiply transitive group is that all the operators of G are included in the two sets H and HSH, S being any operator of G which is not also in H.

When the multipliers $S_2, S_3, \ldots, S_\rho$ in the right co-sets are the same as those in the left co-sets (this is possible for every subgroup of G) two co-sets are said to correspond when they have the same multipliers; that is HS_a and S_aH are two corresponding co-sets. It results from what precedes that this correspondence can be established in only one way when H is invariant under G and it can be established in $(\rho-1)!$ ways when H gives rise to a multiply transitive group. Conversely, when this correspondence can be established in only one way H must be invariant, and K must be multiply transitive whenever it can be established in $(\rho-1)!$ ways.

It should also be observed that the operators of each right co-set are evenly distributed among a certain number of left co-sets whenever they do not all occur in the same left co-set. Similarly the operators of each left co-set must be evenly distributed among the right co-sets. As the transitive constituents of K_1 are not necessarily of the same degrees it results that the operators of two right co-sets are not necessarily distributed among the same number of left co-sets, or vice versa. It may be observed that the method of dividing all the operators of a group into those of a subgroup and the corresponding co-sets was used by Abbati in 1802 and hence it is one of the oldest processes in group theory. This may add interest to the theorem given above in regard to the relation between a multiply transitive representation and the properties of the corresponding co-sets.

§ 2. *Transitive constituents of the subgroup composed of all the substitutions which do not involve a certain letter.*

Suppose that the operators of the right co-set HS_2 are found in the λ left co-sets S_2H, S_3H, . . ., $S_{\lambda+1}H$. The totality of operators HS_2H must therefore give all the operators of these λ left co-set, each operator occurring as many times as there are common operators in H and $S_2^{-1}HS_2$. Hence λ is the index under H of the subgroup composed of these common operators. On the other hand, λ is the degree of the transitive constituent of K_1 which involves the letter replacing a in the substitution corresponding to S_2 in K. Hence *the necessary and sufficient condition that K_1 involves a transitive constituent of degree n_1 is that G involves a substitution which transforms H into a group which has a subgroup of index n_1 in common with H.* In particular, the necessary and sufficient condition that K_1 omits β of the letters contained in K is that H is invariant under a subgroup of G whose order is β times that of H; when $\beta = p$, K is regular and vice versa.

From the theorems proved in the preceding paragraph it is easy to deduce abstract group theory proofs for a number of theorems relating to simply transitive primitive groups. If K is such a group, K_1 is maximal, and if one of the transitive constituents in K_1 is of order p, p being a prime number, K_1 involves an invariant subgroup of index p, as well as a transitive constituent of degree p.

Hence its order is a power of p. As H and $S_2^{-1}HS_2$ have a subgroup of index p in common and as such a subgroup is always invariant in a group whose order is a power of p, it results that these common operators form an invariant subgroup of K. This is impossible unless the order of this common subgroup is unity and hence K, cannot involve a transitive constituent of order p unless the order of K_1 is p.[5]

When K_1 involves a transitive constituent of degree n_1, H and $S_2^{-1}HS_2$ have a subgroup of index n_1 in common and vice versa as was proved above. It is also known that G involves a multiple of n_1h operators which transform H into a group having exactly a subgroup of index n_1 in common with H. It is evident from the above that there are exactly n_1h such operators for every transitive constituent of degree n_1 in K_1. Hence we have the following theorem: *If G involves kn_1h operators which transform H into a group having exactly a subgroup of index n_1 in common with H then must K_1 have exactly k transitive constituents of degree n_1 and vice versa.* In particular, K is multiply transitive when K_1 is transitive and of degree $\rho-1$. Hence the necessary and sufficient condition that K is multiply transitive is that G contains an operator which transforms H into a group which has exactly a subgroup of index $g/h - 1$ in common with H, g and h being the orders of G and H respectively. This theorem gives meaning in certain cases to the theorem, if a subgroup H_1 of a given group G has exactly ρ operators in common with a conjugate of a subgroup H_2 of G, then the number of the operators of G which transform H_2 into subgroups having exactly ρ operators in common with H_1 is $kh_1h_2 \div \rho$, h_1 and h_2 being the orders of H_1 and H_2 respectively. The given theorem gives a meaning to k whenever H_1 and H_2 belong to the same system of conjugates.

From the main theorem of the preceding paragraph it is easy to obtain the degrees of all the systems of intransitivity of K_1. To obtain the orders of the transitive constituents of K_1 it is only necessary to observe that if $S_aHS_a^{-1}$ has a subgroup of index n_1 in common with H and if the largest invariant subgroup of H contained in this common subgroup is of index m_1 under H then the

[5] *Proceedings of the London Mathematical Society*, vol. 28 (1897), p. 536.

corresponding transitive constituent in K_1 is of order m_1 and of degree n_1. The fact that its order is m_1 results directly from the facts that the n_1 right co-sets which involve all the operators of HSH have the property that each of them is unchanged when multiplied on the right by any one of the operators of this invariant subgroup. Moreover, it is evident that the identity of each transitive constituent of K_1 must correspond to an invariant subgroup of K_1. Hence it results that *If H_1, H_2, . . ., H_λ be any complete set of conjugate maximal subgroups of G then each index under any one of these subgroups as regards the largest invariant subgroup which it has in common with any other is divisible by the same prime numbers for every possible pair in the set of conjugate subgroups.*

As a special case of the theorems proved in the preceding paragraph we have the following: The necessary and sufficient condition that K_1 is composed of simply isomorphic transitive constituents is that every invariant subgroup of H which occurs in one of its conjugates under G occurs also in all of these conjugates. This condition must clearly be fulfilled when K_1 is transitive; that is, in this case H cannot have an invariant subgroup in common with any one of its conjugates unless this subgroup is also invariant under G. This theorem exhibits an interesting abstract group property which corresponds to the property that K_1 is composed of simply isomorphic transitive constituents and with those mentioned above establishes more completely the principle of duality as regards substitution groups and abstract groups.

§ 3. *Transitive representation as regards right and left co-sets.*

Since both the right and the left co-sets of G are determined by the subgroup H each of these two categories of co-sets together with H forms a totality whose elements are permuted among themselves when the former are multiplied on the right and the latter on the left by operators of G. The ρ sets obtained by adding H to the right co-sets will be called the *augmented* right co-sets. Similarly we shall use the term augmented left co-sets for the ρ sets obtained by adding H to the left co-sets. It is known, and also evident, that the permutations among themselves obtained by multiplying the augmented right co-sets on the right successively by all the operators

of G constitute a substitution group K which is simply isomorphic to the quotient group of G with respect to the largest subgroup of H which is invariant under G.

To see very clearly the relation between G and K it is perhaps best to assume at first that they are simply isomorphic. We shall represent by K_1 the subgroup of G which corresponds to H in the simple isomorphism between G and K. Hence K_1 is also composed of all the substitutions of K which omit a given letter a, as was observed in the preceding section. As each of the co-sets is composed of all the substitutions of K which replace a by a particular letter we may name each of these co-sets by this particular letter. In particular, K_1 will be represented by a. If this is done it is evident that the permutations of the augmented co-sets due to multiplying all these co-sets on the right by the same substitution will be identical with this substitution. That is, the substitutions of K will only be repeated by the permutations of the augmented right co-sets when all of them are multiplied on the right by all the substitutions of K. That this arrangement was possible is a direct consequence of the manner in which K was constructed, the details which we gave are intended to exhibit more clearly how this may be done.

We proceed to consider the substitution group K' which corresponds to the permutations of the augmented left co-sets when these are multiplied successively on the left by all the substitutions of K, in order. We again suppose that K_1 corresponds to H, and that it is composed of all the substitutions of K which omit a. The left co-sets are composed separately of all the substitutions of K which replace a particular letter by a. We shall name each of these co-sets by this particular letter and hence H will again be denoted by a. Multiplying each one of these augmented left co-sets on the left by the separate substitutions of K gives a permutation of these co-sets represented by the inverse of the multiplying substitution. Hence we again obtain a repetition of all the substitutions of K if we consider the permutations of the augmented left co-sets when these are multiplied on the left by all the substitutions of K in order.

From the preceding paragraphs it results that the right and left

augmented co-sets may be so named respectively that there results the same substitution group when the left augmented co-sets are multiplied on the left as when the right augmented co-sets are multiplied on the right. When H is invariant under G K is regular, and K and K'' are each composed of all the substitutions on these letters which are separately commutative with every substitution of the other, K'' being obtained by left-hand multiplication when the co-sets (which reduce to single operators in this case) are named the same as in the right co-set. As K'' reduces to K when these co-sets are named in the manner noted above it results from what has been proved that K and K'' are conjugate. When K is composed of substitutions of order two in addition to the identity, the two given methods of naming the co-sets will coincide and hence the given process also gives, as a special case, a proof of the theorem that every group in which all the substitutions besides the identity are of order 2 must be abelian. It should be added that the main results of this section are not new but the subject is so important that these details should be of some interest as they throw new light on the entire process.

UNIVERSITY OF ILLINOIS,
May, 1910.